LISTING OF CLAIMS

The listing of claims provided below replaces all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for using a smart card ~~token~~ to authenticate a downloaded ~~sign an~~ unsigned binary, comprising:

signing an unsigned binary on a first computing device to generate ~~obtain~~ a first signature;

downloading said first signature and said unsigned binary to a temporary buffer on a second computing device;

interfacing a smart card with said second computing device such that the smart card has access to said temporary buffer;

operating said smart card to read said first signature and said unsigned binary from said temporary buffer;

operating said smart card to sign said unsigned binary using a secret key present on said smart card ~~using a token coupled to said second computing device to sign said unsigned binary~~ to generate ~~obtain~~ a second signature; and

operating said smart card to compare ~~comparing~~ said first and second signatures,

wherein a common signing methodology is used on both said first computing device and said smart card to respectively generate said first and second signatures, and wherein said secret key present on said smart card is not accessible by said second computing device.

2. (Currently Amended) The method of claim 1, further comprising:

using said unsigned binary on said second computing device, if said smart card determines that said first and second signatures match.

3. (Currently Amended) The method of claim 1, further comprising:

rejecting said unsigned binary on said second computing device, if said smart card determines that said first and second signatures do not match.

4. (Cancelled)

5. (Currently Amended) The method of claim 1, wherein said first computing device is a server.

6. (Currently Amended) The method of claim 1, wherein said common signing methodology utilizes a hash algorithm ~~steps of signing and using use identical hashes~~.

7. (Currently Amended) The method of claim 1, further comprising:

encrypting said unsigned binary and said first signature.

8. (Currently Amended) The method of claim 7, further comprising:

decrypting ~~de-crypting~~ said encrypted unsigned binary and first signature.

9. (Currently Amended) A computer readable medium having program instructions encoded therein for using a smart card to authenticate a downloaded ~~program product, comprising:~~

~~a computer usable medium having computer readable program code embodied therein configured to use a token to sign an~~ unsigned binary, ~~said computer program product~~ comprising:

program instructions for signing ~~computer readable code configured to cause a computer to sign~~ an unsigned binary on a first computing device to generate ~~obtain~~ a first signature;

program instructions for downloading ~~computer readable code configured to cause a computer to download~~ said first signature and said unsigned binary to a temporary buffer on a second computing device;

program instructions for interfacing a smart card with said second computing device such that said smart card has access to said temporary buffer;

program instructions for operating said smart card to read said first signature and said unsigned binary from said temporary buffer;

program instructions for operating said smart card ~~computer readable code configured to cause a computer to use a token coupled to said second computing device~~ to sign said unsigned binary using a secret key present on said smart card to generate ~~obtain~~ a second signature; and

program instructions for operating said smart card ~~computer readable code configured to cause a computer~~ to compare said first and second signatures,

wherein a common signing methodology is used on both said first computing device and said smart card to respectively generate said first and second signatures, and wherein said secret key present on said smart card is not accessible by said second computing device.

10. (Currently Amended) The computer readable medium ~~program product~~ of claim 9, further comprising:

program instructions for directing said second computing device ~~computer readable code configured to cause a computer~~ to use said unsigned binary on said second computing device, if said first and second signatures match.

11. (Currently Amended) The computer readable medium ~~program product~~ of claim 9, further comprising:

program instructions for directing said second computing device ~~computer readable code configured to cause a computer~~ to reject said unsigned binary on said second computing device, if said first and second signatures do not match.

12. (Cancelled)

13. (Currently Amended) The computer readable medium ~~program product~~ of claim 9, wherein said first computing device is a server.

14. (Currently Amended) The computer readable medium ~~program product~~ of claim 9, wherein said common signing methodology utilizes a hash algorithm ~~computer readable code configured to cause a computer to use and said computer readable code configured to cause a computer to sign use identical hashes~~.

15. (Currently Amended) The computer readable medium ~~program product~~ of claim 9, further comprising:

program instructions for encrypting ~~computer readable code configured to cause a computer to encrypt~~ said unsigned binary and said first signature.

16. (Currently Amended) The computer readable medium ~~program product~~ of claim 15, further comprising:

program instructions for decrypting ~~computer readable code configured to cause a computer to de-crypt~~ said unsigned binary and said first signature.